REMARKS

Applicants submit the present Amendment to respond to the Office Action mailed August 11, 2006.

I.   The Claim Amendments

Applicants have made clarifying amendments to independent Claims 1, 9 and 18. While Applicants submit that the present application makes clear that the "computer-actionable Threat Management Vector (TMV)" of Claims 1, 9 and 18 is a vector that is in a form that is suitable for use by an **automated** threat management system, in the Office Action it appears that the TMV has been interpreted as covering any computer-**readable** file, such as an e-mail message or a report generated on a word processing system. (*See* Office Action at p. 3, ¶ 3.1, stating that reports which are sent in the form of a file are "a computer actionable item, containing fields reflecting different information items"). Applicants respectfully submit that this interpretation is incorrect, as the present specification makes clear that "embodiments of the present invention can consolidate the human interpretation of threat management information to a single point, establish an unambiguous representation of the information using a common semantic information base, and produce a computer-actionable message unit that is suitable for use by an automated threat management system." (Specification at p. 5, lines 7-12; *see also* Specification at p. 16, lines 17-23). In any event, in order to clarify the scope of the claims, independent Claims 1, 9 and 18 have each been amended to recite that the TMV is in a format "suitable for use by an automated threat management system." Support for these amendments may be found, for example, at the above identified excerpts from the original Specification.

II.   The Rejections Under 35 U.S.C. § 102

Claims 1-23 stand rejected as anticipated under 35 U.S.C. § 102(e) by U.S. Patent Application Publication No. 2003/0084349 to Friedrichs et al. ("Firedrichs"). (Office Action at p. 2, ¶ 3). Applicants respectfully traverse these rejections.

Friedrichs is directed to an "early warning system for network attacks." (Friedrichs at Title). In the system/methods of Friedrichs, a plurality of security devices record information relating to security events that occur across a network. (*See, e.g.*, Friedrichs at ¶ 17). Some of

this information is then extracted and written into a file having a common format. (*See, e.g.,* Friedrichs at ¶ 18). The information may then be transferred to a database server, where it may be converted into a common, vendor-independent format and analyzed. (*See, e.g.,* Friedrichs at ¶¶ 19 and 23-24). Finally, reports may be generated based on the analyzed data, and these reports are made available to users. (*See, e.g.,* Friedrichs at ¶ 25). The information provided to the user "may contain reports, graphs of security event data and other information related to the processing and analysis of security events and the detection of security incidents", user-requested "specific reports . . . on event data" and/or a "set of reports outlining recent abnormal activity." (Friedrichs at ¶ 26). The reports may be made available to users via a web server, e-mail, pager, facsimile or other delivery mechanisms. (*See, e.g.,* Friedrichs at ¶ 25).

Applicants respectfully submit that Friedrichs is simply another example of the labor-intensive prior art security threat management systems described in the background section of the present application. User's of the system –i.e., individuals – of Friedrichs are provided written reports containing processed security event data. Each such user must then determine how to respond to the security threats contained within the reports and implement such responses. This is exactly the labor-intensive intervention process that embodiments of the present invention avoid. Thus, as discussed in more detail below, Applicants respectfully submit that Friedrichs does not anticipate any of the pending claims and, consequently, Applicants respectfully request withdrawal of the pending rejections.

A.   The Rejection of Claim 1

Claim 1, as amended, recites:

> 1.   A method of generating computer security threat management information, comprising:
>
> receiving notification of a computer security threat;
>
> generating a computer-actionable Threat Management Vector (TMV) that is suitable for use by an automated threat management system from the notification that was received, the TMV including therein a first computer-readable field that provides identification of at least one system type that is affected by the computer security threat, a second computer-readable field that provides identification of a release level for the

system type and a third computer-readable field that provides identification of a set of possible countermeasures for a system type and a release level; and

transmitting the computer-actionable TMV that is generated to a plurality of target systems for processing by the plurality of target systems.

As should be clear from the discussion above, Friedrichs does not disclose "generating a **computer-actionable** Threat Management Vector (TMV) that is **suitable for use by an automated threat management system**" as recited in Claim 1. Instead, the identified "TMV" of Friedrichs is a report that outlines security event activity that led to the alert and may contain graphs that depict relevant security event data. (*See, e.g.,* Friedrichs at ¶ 39). Such a report is not "computer-actionable", nor is it "suitable for use by an automated threat management system." Applicants also respectfully submit that Friedrichs does not disclose a TMV having first, second and third "computer-readable fields" that contain the specific information specified in Claim 1. In computer science, a "field" is commonly known to refer to a separately-accessible sub-unit of data that has several parts. (*See, e.g.,* wikipedia.com, stating "In computer science, data that has several parts can be divided into fields. For example, a computer may represent today's date as three distinct fields: the day, the month and the year."). Applicants respectfully submit that there is no indication that the reports discussed in Friedrichs include the first, second and third fields of Claim 1. Thus, the rejection of Claim 1 should be withdrawn for at least these reasons.

In addition, Applicants respectfully submit that the cited portions of Friedrichs do not disclose including in a TMV (1) a field that provides identification of at least one **system type that is affected by** the computer security threat or (2) a field that provides identification of a **release level** for the system type. In particular, the Office Action cites to paragraphs 42 and 35 of Friedrich as disclosing providing "identification of at least one system type that is affected by the computer security threat." (Office Action at p. 3, ¶ 3.1). However, what the cited portion of Friedrichs discloses is a Sensors database **405** that contains demographic information about the location, type and/or operating system of **the security devices that uploaded information** into the All-Events database or reported the security event, as opposed to identification of the "system type that is **affected by the computer security threat**" as recited in Claim 1. Applicants

respectfully submit that the fact that a security device **reports** a security event does not mean that the reporting security device is **affected by** the computer security threat. The Office Action likewise cites to paragraph 42 of Friedrich as disclosing providing "identification of a release level for the system type." (Office Action at p. 3, ¶ 3.1). However, once again the "type" information relates to the type of security device that is uploading information as opposed to the type of device that is affected by the security threat, and there is no indication that any "release" information is even provided. Thus, the rejection of Claim 1 should also be withdrawn for these additional reasons.

Applicants further submit that the cited portions of Friedrichs do not disclose including a field in a TMV that "provides identification of a set of possible countermeasures for a system type and a release level." The Office Action cites to paragraph 35 of Friedrichs as disclosing this recitation of Claim 1; however, the cited portion of Friedrichs merely describes the types of demographic information that may be provided. There is absolutely no disclosure or suggestion of including a set of possible countermeasures for the particular system type and release level. Accordingly, for each of the above reasons, Applicants respectfully submit that Friedrichs does not anticipate Claim 1, and hence respectfully request that the rejection of Claim 1 be withdrawn.

B.   The Rejections of Claims 2-8

Claims 2-8 depend from Claim 1 and hence are patentable for at least the reasons, discussed above, that Claim 1 is patentable over Friedrichs. In addition, Applicants submit that at least Claims 2-6 are separately patentable over Friedrichs.

Claim 2 recites "selecting a system type, release level and possible countermeasures from a database that lists system types, release levels and possible countermeasures in a computer-readable format." The Office Action cites to paragraphs 40-46 of Friedrichs as disclosing the recitations of Claim 2; however, the cited portions of Friedrichs make no mention of selecting system type, release and possible countermeasures from a database and then converting this information into a computer-readable format for inclusion in a TMV. Accordingly, Claim 2 is independently patentable over Friedrichs.

Claim 3 recites that the "system type comprises a computer operating system type" and that "the release level comprises a computer operating system release level." The Office Action cites to paragraphs 35 and 42 of Friedrichs as disclosing the recitations of Claim 3; however, the cited portions of Friedrichs make no mention of the release level as recited in Claim 3. Accordingly, Claim 3 is also independently patentable over Friedrichs.

Claim 4 recites that "the set of possible countermeasures comprises an identification of a countermeasure mode of installation." The Office Action cites to paragraph 45 of Friedrichs as disclosing the recitations of Claim 4. However, paragraph 45 of Friedrichs discusses a separate Vulnerabilities database 440 and a Product database 450. The product database may include details on how to patch a particular flaw. However, there is no indication that the information in the Products database is in a computer-actionable format, and it is clear that the information in the Products database 450 is not part of the report (i.e., the alleged TMV) that is sent to the users. Accordingly, Claim 4 is also independently patentable over Friedrichs.

Claim 5 recites that least one of the identifications comprises a pointer. The Office Action states that "pointers are broadly used in databases to identify data," implicitly conceding that the recitation of Claim 5 is not disclosed in Friedrich. Moreover, assuming, for the sake of argument, that pointers are broadly used in databases, the alleged TMV in Friedrichs is not a database, but a report. For each of these reasons Applicants submit that Claim 5 is also independently patentable over Friedrichs.

Claim 6 recites that the TMV further includes "a fourth computer-readable field that provides identification of at least one subsystem type that is affected by the computer security threat and a fifth computer-readable field that provides identification of a release level for the subsystem type, the third computer-readable field providing identification of a set of possible countermeasures for a subsystem type and a release level." Applicants respectfully submit that Friedrichs does not discuss types and/or release levels of subsystems, and hence likewise does not anticipate Claim 6 for this additional reason.

C.   The Rejections of Claims 9-23

In re: Bardsley et al.
Application No.: 10/624,344
Filed: July 22, 2003
Page 11

Claims 9-23 stand rejected based on the same rationale as Claims 1-8. Accordingly, Applicants respectfully submit that the rejections of these claims should be withdrawn for at least the same reasons, discussed above, that the rejections of Claims 1-8 should be withdrawn.

III.   Conclusion

Inasmuch as the points and concerns raised in the Office Action have been addressed in full, Applicants respectfully request that this application is in condition to pass to issue, which action is respectfully requested. Should the Examiner have any matters of outstanding resolution, he is encouraged to telephone the undersigned at 919-854-1400 for expeditious handling.
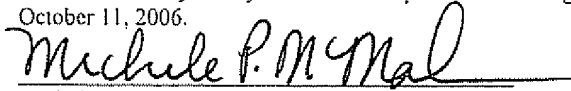
Respectfully submitted,

D. Randal Ayers
Registration No. 40,493

Customer No. 46590
Myers Bigel Sibley & Sajovec
P. O. Box 37428
Raleigh, North Carolina 27627
Telephone: (919) 854-1400
Facsimile: (919) 854-1401